October 8 2003

# INTERIM SENSITIVE SECURITY INFORMATION (SSI) POLICIES AND PROCEDURES FOR SAFEGUARDING AND CONTROL

---

1. PURPOSE. To specify the requirements that must be implemented immediately by all employees and contractors covered under paragraph 3 of this document to mark, store, control, transmit, destroy, and manage the release or withholding of Sensitive Security Information (SSI). This policy covers SSI in every form in which it is stored, including paper, electronic, magnetic, and other media. This policy contains the minimum standards for employees and contractors to mark, store, control, transmit, and destroy SSI.

2. BACKGROUND. Sensitive Security Information is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined by the Administrator that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation. Although it is subject to certain legal disclosure limitations, SSI is not classified national security information subject to the handling requirements governing classified information.

The specific information that falls within the scope of the statute is prescribed by regulation at 49 CFR 1520. The purpose of this provision is to prevent unauthorized disclosure of information that could cause any of the harms listed above, while being mindful of the public's legitimate interest in, and right to know, transportation information. Limiting access to this information is necessary to guard against those who pose a threat to transportation security and their ability to develop techniques to subvert security measures.

3. SCOPE. This policy memorandum prescribes direction to Federal employees and contractors regarding the control, safeguarding, and release of SSI in all of its paper, electronic, magnetic, and other forms. All TSA contracts must include provisions requiring contractors to handle SSI in accordance with this interim guidance.

4. Designation Authority for SSI. The Administrator has the authority to designate information as SSI. Appendix 1 identifies the types of documents/information that are currently designated as SSI. Information not designated as SSI in 49 CFR 1520.7(a) through (j) and (l) through (r) will be categorized as SSI only upon a written determination by the Administrator that such categorization is necessary in the interest of the safety of persons in transportation. Offices wishing to have additional information designated as SSI must make this request in writing to the Administrator.

5. DEFINITIONS.

a. Sensitive Security Information (SSI). Records and information specified in 49 CFR 1520.7 (a) through (r). See Appendix 1, Sensitive Security Information (SSI).

b. SSI Distribution Limitation Statement. The statement that is applied to SSI that provides explicit direction concerning the restrictions which apply to the information or records. It states the authority for controlling distribution and specifies, when appropriate, the distribution approval procedures.

c. Need to Know Federal Employees and Contractor Employees - A Federal employee has a need to know SSI when access to the information is necessary for the employee to accomplish official duties. A contractor employee has a need to know SSI when access to the information is necessary for the employee to carry out a requirement of a Federal contract relating to transportation security.

d. Need to Know - Regulated Parties and others. For specific SSI, the designation authority may make a finding that only specific persons or classes of persons have a need to know. Otherwise, a regulated party has a need to know SSI in each of the following circumstances:

(1) When the person needs the information to carry out transportation security duties.

(2) When the person needs the information to supervise or otherwise manage individuals carrying out transportation security duties.

(3) When the person needs the information to advise an operator, carrier, or other affected entity regarding transportation security duties.

(4) When the person needs the information to represent an operator, carrier, or other person receiving information under the provisions of section 1520.3(d) in connection with any enforcement proceedings.

e. Record. Includes any writing, drawing, map, tape, film, photograph, or other means by which information is preserved, regardless of format. This includes paper, electronic, and magnetic media.

## SECTION 1 - PROTECTIVE MARKING AND LIMITED DISTRIBUTION STATEMENT FOR SSI

6. RESPONSIBILITY. A person who creates a record containing SSI must, in accordance with this section, include a protective marking and limited distribution statement that clearly identifies the information as SSI and specifies the distribution limitation required. A person who receives a record containing SSI that is not marked in accordance with this section must apply such marking and inform the sender of its omission.

7. REQUIREMENTS FOR PROTECTIVE MARKING AND LIMITED DISTRIBUTION STATEMENT.

a. Protective Marking. The protective marking consisting of the words "**SENSITIVE SECURITY INFORMATION"** must be applied to all documents that contain SSI. This marking should be written or stamped in plain style bold type, Times New Roman and a font size of 16, or an equivalent style and font size.

b. Distribution Limitation Statement. The distribution limitation statement must be applied to all documents that contain SSI. This statement should be written or stamped in plain style bold type, Times New Roman and a font size of 8, or an equivalent style and font size.

**"WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552."**

8. Marking Requirements For SSI Documentation. These marking requirements apply to all records containing SSI that are created subsequent to the date of this policy memorandum, and to all existing records containing SSI, prior to their release.

a. Documents.

(1) Protective Marking. The protective marking must be applied at the top of the outside of any front cover (including a binder or folder), on the top of any title page, on the top of the first page and each subsequent page, and on the top of the outside of any back cover (including a binder or folder).

(2) Distribution Limitation Statement. The distribution limitation statement must be applied at the bottom of the outside of any front cover (including a binder or folder), on the bottom of any title page, on the bottom of the first page and each subsequent page, and on the bottom of the outside of any back cover (including a binder or folder).

b. Charts, Maps and Drawings.

(1) Protective Marking. Charts, maps, and drawings designated as SSI must have the appropriate protective markings affixed in a manner that it is plainly visible.

(2) Limited Distribution Statement. Charts, maps, and drawings must have the appropriate distribution limitation statement affixed in a manner that it is plainly visible.

c. Motion Picture Films and Video Recordings.

(1) Protective Marking and Distribution Limitation Statement. The protective marking and distribution limitation statement must be applied at the beginning and end of each reel and affixed in such a manner that it is fully visible on the screen or monitor.

(2) Motion Picture Reels. Motion picture reels that are kept in film cans or other containers must have protective markings and distribution limitation statements. The protective marking and distribution limitation statements must be applied to each side of each reel and to all sides of each can or other storage container. In addition to reproducing the protective marking and distribution limitation statement on the beginning and end portions of the film, if the motion picture film has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement must, if practicable, be included in the introduction and at the end of the film.

(3) Videotape Recordings. Videotape recordings that contain SSI must include on the recordings conspicuous visual protective markings and distribution limitation statements at both the beginning and the end, if practicable. Protective markings and the distribution limitation statement must also be applied on the front and back and on each side of the video case and storage containers.

d. Electronic and Magnetic Media

(1) Information Extracted from. The SSI protective marking is not required on information in the form of compiled lists of SSI information extracted from electronic and magnetic media. However, information in the form of compiled lists of SSI information extracted from electronic and magnetic media must have the distribution limitation statement affixed on the bottom of the each page containing SSI, and to any cover page and back page. The distribution limitation statement may be applied by the equipment itself on the face of the page provided the distribution limitation statement is clearly distinguishable from the printed text.

(2) Information Contained on. SSI contained on electronic and magnetic media must have protective markings and the distribution limitation statement applied at the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement must be displayed in such a manner that both are fully visible on the screen or monitor when the text is viewed. The protective marking and distribution limitation statement must also be applied to each side of the disk and the disk sleeve/jacket, on the non-optical side of the CD-ROM and both sides of the CD-ROM case. If the electronic/magnetic text has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement must, if possible, be included in the introduction and at the end of this text.

9. TRANSMITTAL DOCUMENTS. Documents that are used to transmit SSI but do not themselves contain SSI must be marked with the distribution limitation statement. In addition, the following statement must be affixed to the front page of the transmittal document.

**"The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."**

## SECTION 2 - STORAGE OF SSI

10. REQUIREMENT. All Federal employees and contractor employees possessing SSI are responsible for ensuring that the information and records containing SSI are safeguarded at all times from disclosure to unauthorized personnel. When the SSI for which an individual is responsible is not under the individual's direct physical control, the individual is responsible for ensuring that it is safeguarded and protected in such a way that it is not physically or visually accessible to persons who do not have a need to know, as defined in paragraph 5 above. For example: when unattended, SSI must be secured in a locked container or office, or other restricted access area.

11. KEY AND COMBINATION CONTROL. When an individual responsible for SSI places the material in a locked container, the individual is responsible for ensuring that positive measures are in force to restrict access to the container keys or combination to only individuals with a need to know.

## SECTION 3 - CONTROL AND RELEASE OF SSI

12. AUTHORITY TO RELEASE AND/OR WITHHOLD SSI DOCUMENTS / INFORMATION. Except as provided in paragraph 13, below, the authority to release SSI to persons who do not have a need to know is limited to the designation authority and any other individual formally designated to act in that capacity.

13. FREEDOM OF INFORMATION ACT (FOIA) REQUESTS. Under 49 U.S.C. 40119, information designated as SSI under part 1520 qualifies for exemption from disclosure under the FOIA based on exemption 3, 5 U.S.C. 552(b)(3).

a. Authority to Deny FOIA Requests. FOIA requests for SSI are processed by the appropriate DOT agency/entity (see, 49 CFR Part 7), except that any decision to release SSI must have the concurrence of the Administrator.

b. Information Requests Received by Regulated Parties. Requests for information that are addressed to regulated parties, such as under State and local freedom of information or open records acts, are addressed in 49 CFR section 1520.5(a), which provides that requests for SSI be referred to the Administrator. TSA works with operators, carriers, and other affected entities to determine what records or portions of records should remain undisclosed and what may be released.

c. Release of Records containing both SSI and Non-SSI. If a record contains information that may not be disclosed under part 1520, but also contains information that may be disclosed, the latter information will be provided in response to a FOIA request, provided the record is not otherwise exempt from disclosure under FOIA, if it is practical to redact the requested information from the record. If it is not practical to do so, the entire record will be withheld from public disclosure.

14. CONTRACTOR ACCESS TO SSI. Prior to a contractor gaining access to SSI, the contractor must meet the processing requirements established by TSA. (These requirements are being developed and will be added as an appendix to this document at a later date. In the interim, contractors will be bound by non-disclosure agreements and any other limitations in their contracts.)

15. CONTROL AND RELEASE OF CONTRACTOR COPIED SSI. Contractors must provide prior notification in writing, through the Contracting Officer, to the originator of SSI when the contractor needs to make copies of SSI. This written notification must contain the following minimum information:

a. Positive identification of SSI (title, document numbers as applicable, etc.).

b. Purpose for making the copies.

c. Quantity of copies.

d. Dissemination of copies (the contractor must verify and ensure that all recipients are authorized to receive SSI.).

16. RELEASE OF SSI TO GOVERNMENT OFFICIALS/EMPLOYEES AND REGULATED PARTIES. Release of SSI is permitted to federal, state and municipal government officials/employees and regulated parties who have a need to know as established by regulation or authorized by the Administrator.

17. RELEASE OF SSI TO LOCAL LAW ENFORCEMENT OFFICIALS AND FEDERAL INTELLIGENCE AGENCIES. Release of SSI is permitted to federal, state and local law enforcement officials, or to federal intelligence agencies who have a need to know as established by regulation or authorized by the Administrator.

18. REQUESTS FOR SSI FROM A FOREIGN GOVERNMENT AND/OR OTHER FOREIGN OR INTERNATIONAL ENTITY. Requests for SSI must be referred to the Administrator.

19. OTHER REQUESTS FOR SSI. Requests for SSI other than under paragraphs 13, 15, 16, 17and 18, above, must be referred to the Administrator.

20. INADVERTENT RELEASE OF SSI. An employee with knowledge of an inadvertent release of SSI must immediately notify the originating authority.

## SECTION 4 - PACKAGING AND TRANSMITTING SSI

21. RESPONSIBILITY. The term “SSI transmission” refers to the means used to transfer SSI from one location to another. A transfer may involve the physical relocation, or the electronic transmission of information. In either case, the individual responsible for the SSI is also responsible for ensuring that the material is packaged and/or transmitted in accordance with the requirements in this guidance.

22. PACKING AND TRANSMISSION REQUIREMENTS FOR SSI. When assembling a package containing SSI for transmission, it is the responsibility of the individual preparing the package to ensure that all SSI has the appropriate protective markings and distribution limitation statements.

a. Mail. SSI may be transmitted by U.S. Postal Service first class mail or regular parcel post, or by other delivery services (Federal Express, UPS, etc). SSI that is to be sent by mail or by a delivery service must be wrapped in opaque envelopes, wrappings, or cartons. Addressing the package with an attention line containing the name and office of the recipient helps to ensure that the SSI material is received and opened only by authorized personnel.

b. Interoffice mail. When sent by interoffice mail, SSI must be transmitted in a sealed envelope in such a manner as to prevent inadvertent visual disclosure.

c. Hand carrying within or between buildings. SSI that is carried by hand within or

between buildings must be protected (by a cover sheet, protective folder, distribution pouch, etc.) to prevent inadvertent visual disclosure.

d. Packaging material. Envelopes or containers must be of such strength and durability that they will provide physical protection during transit and will prevent items from breaking out of the containers or envelops.

23. ELECTRONIC TRANSMISSION OF SSI. When transmitting SSI over telecommunications circuits, the following procedures apply.

a. Electronic Mail or Web Posting. SSI transmitted by e-mail must be in a password-protected attachment. SSI is not authorized for posting on the internet/intranet except for postings on secure sites as specifically authorized by the Administrator. (see, Appendix 2).

b. Facsimile.

(1) The sender must confirm that the facsimile number of the recipient is current and valid.

(2) If the recipient has a facsimile machine in a controlled area where unauthorized persons cannot intercept the SSI facsimile, the sender may send the SSI facsimile without requiring that the recipient be there to receive it promptly. Otherwise, the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information.

(3) The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

c. Telephone. The caller must ensure that the person receiving the SSI is an authorized recipient. The risk of interception and monitoring of conversations is greater when using cellular telephones and cordless telephones, which transmit the conversation to a base unit. Individuals needing to pass SSI by telephone must avoid these devices unless the circumstances are exigent, or the transmissions are encoded or otherwise protected.

## SECTION 5 - DESTRUCTION OF SSI

24. REQUIREMENT. When copies of records containing SSI are no longer needed, they must be promptly and completely destroyed.

25. METHODS. The objective of a selected destruction method is to destroy the material so that recovery of the sensitive information is difficult, if not impossible. Material containing SSI must be destroyed by one of the following methods, listed in order of preference:

a. Any means approved for the destruction of national security classified material as specified in applicable orders regarding the destruction of national security classified material. The approved means include burning, pulping, crosscut shredding, melting, chemical decomposition and mutilation. Because of the potential hazards posed to employees and the environment by melting, chemical decomposition, and mutilation, use of any of these methods must be carefully considered.

b. Tearing it into small pieces and assimilating it with other waste material. When destroying SSI by hand, it must be cut or torn into pieces measuring not more than 1/2 inch on a side, and mixed with other wastepaper material in the process.

26. CONTRACTOR NOTIFICATION OF DESTRUCTION OF SSI. When a contractor proposes to destroy copies of records containing SSI, the contractor must first provide notification in writing, through the Contracting Officer, to the information originator of its destruction. The contractor must provide the following minimum information regarding the destruction of SSI:

a. Identification of the information to be destroyed, (title, document/copy numbers(s) as applicable, etc.).

b. Quantities of copies destroyed.

c. Date and place of destruction.

d. Method of destruction.

e. Residual SSI remaining in custody of the contractor.

## APPENDIX 1

## SENSITIVE SECURITY INFORMATION (SSI)

1. GENERAL. Except as otherwise provided in writing by the designation authority as necessary in the interest of the safety of persons in transportation, this appendix lists the information and records containing such information that constitute SSI as listed in 14 CFR 1520.7.

2. INFORMATION CONSTITUTING SSI.

(a) Any approved, accepted, or standard security program under the rules listed in §1520.5(a)(1) through (6), and any security program that relates to United States mail to be transported by air (including that of the United States Postal Service and of the Department of Defense); and any comments, instructions, or implementing guidance pertaining thereto.

(b) Security Directives and Information Circulars under §1542.303 or §1544.305 of this chapter, and any comments, instructions, or implementing guidance pertaining thereto.

(c) Any selection criteria used in any security screening process, including for persons, baggage, or cargo under the rules listed in §1520.5(a)(1) through (6).

(d) Any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto under the rules listed in §1520.5(a)(1) through (6).

(e) Technical specifications of any device used for the detection of any deadly or dangerous weapon, explosive, incendiary, or destructive substance under the rules listed in §1520.5(a)(1) through (6).

(f) A description of, or technical specifications of, objects used to test screening equipment and equipment parameters under the rules listed in §1520.5(a)(1) through (6).

(g) Technical specifications of any security communications equipment and procedures under the rules listed in §1520.5(a)(1) through (6).

(h) As to release of information by TSA: Any information that TSA has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack. This includes, but is not limited to, details of inspections, investigations, and alleged violations and findings of violations of 14 CFR parts 107, 108, or 109 and 14 CFR 129.25, 129.26, or 129.27 in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001); or parts 1540, 1542, 1544,

1546, 1548, or §1550.5 of this chapter, and any information that could lead the disclosure of such details, as follows:

(1) As to events that occurred less than 12 months before the date of the release of the information, the following are not released: the name of an airport where a violation occurred, the regional identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of the aircraft operator in connection with specific locations or specific security procedures. TSA may release summaries of an aircraft operator's total security violations in a specified time range without identifying specific violations. Summaries may include total enforcement actions, total proposed civil penalty amounts, total assessed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(2) As to events that occurred 12 months or more before the date of the release of information, the specific gate or other location on an airport where an event occurred is not released.

(3) The identity of TSA or FAA special agent who conducted the investigation or inspection.

(4) Security information or data developed during TSA or FAA evaluations of the aircraft operators and airports and the implementation of the security programs, including aircraft operator and airport inspections and screening point tests or methods for evaluating such tests under the rules listed in §1520.5(a)(1) through (6).

(i) As to release of information by TSA: Information concerning threats against transportation.

(j) Specific details of aviation security measures whether applied directly by the TSA or entities subject to the rules listed in §1520.5(a)(1) through (6). This includes, but is not limited to, information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations.

(k) Any other information, the disclosure of which TSA has prohibited under the criteria of 49 U.S.C. 40119.

(l) Any draft, proposed, or recommended change to the information and records identified in this section.

(m) The locations at which particular screening methods or equipment are used under the rules listed in §1520.5(a)(1) through (6) if TSA determines that the information meets the criteria of 49 U.S.C. 40119.

(n) Any screener test used under the rules listed in §1520.5(a)(1) through (6).

(o) Scores of tests administered under the rules listed in §1520.5(a)(1) through (6).

(p) Performance data from screening systems, and from testing of screening systems under the rules listed in §1520.5(a)(1) through (6).

(q) Threat images and descriptions of threat images for threat image projection systems under the rules listed in §1520.5(a)(1) through (6).

(r) Information in a vulnerability assessment that has been authorized, approved, or funded by DOT, irrespective of mode of transportation.

## APPENDIX 2

## THE ELECTRONIC POSTING/TRANSMISSION OF SENSITIVE SECURITY INFORMATION (SSI)

1. WEB POSTING. All SSI information can only be posted on TSA approved web sites. Such sites must be approved by and comply with the standards established by the Office of Information Security, in the office of the Chief Information Officer (CIO), and authorized by the Administrator. Neither the TSA internet nor the internal intranet are presently approved for posting SSI material. However, the CIO's office has authorized limited secure intranet web sites for this purpose. For questions regarding such web sites and their usage, please send your e-mail inquiries to tsa-content@tsa.dot.gov.

2. ELECTRONIC TRANSMISSION. All SSI information transmitted via e-mail must be password protected via standards established by the Office of Information Security (InfoSec), in the office of the Chief Information Officer (CIO). InfoSec has authorized the continued use of Microsoft word and data processing software provided the standards for password protection listed under sec.(a) are used.

a. Minimum standards for transmission between TSA employees.

(1) Password criteria. Passwords used shall conform to the following guidelines

- eight character minimum length,
- at least one letter capitalized,
- contain at least one number,
- not be a word in the dictionary.

(2) Duration and Usage. Passwords shall have a working life of no more than ninety (90) days from creation. Passwords may be applied to multiple documents between the sender/receiver(s) for those days.

(3) Communicating Passwords. Sender shall transmit password to receiver(s) by alternate means other than e-mail, i.e. telephone or fax. Use of cellular or cordless phones is restricted as provided under paragraph 21(c).

(4) Non-Applicability for Classified Information. This procedure shall not be used for transmission of classified information.

(5) Password Creation. System owners are responsible for password creation and maintenance.

b. Administration of Passwords

(1) One common password, subject to the 90 day limitation of paragraph 2(a)(2) of this appendix, is authorized for all SSI documents transmitted between TSA employees.

(2) A separate but common password, subject to the 90 day limitation of paragraph 2(a)(2) of this appendix, is authorized for all SSI documents transmitted to non-TSA employees with a need to know.

(3)The office of Security Regulation and Policy will establish the common passwords in accordance with section 2(a) of this appendix. TSA employees should direct any questions regarding passwords to their individual organizations.